CLAIMS

1. A method in connection with a first computing device ('transmitter') and a second computing device ('receiver') interconnected by a network, the transmitter for transmitting protected digital content to the receiver in a manner so that the receiver can access the content, the content being encrypted and decryptable according to a content key (KD), the method comprising:

the receiver sending a session request to the transmitter, the session request including an identification of the content to the transmitter, an action to be taken with the content, and a unique identification of the receiver;

the transmitter receiving the session request from the receiver, determining from the unique identification of the receiver in the session request that the receiver is in fact registered to the transmitter, obtaining a digital license corresponding to the identified content in the session request, reviewing policy set forth in the license to determine that the license allows the transmitter to provide access to the content to the receiver and also allows the action in the session request, and sending a session response to the receiver, the session response including the policy from the license, the unique identification of the receiver, and the content key (KD) for decrypting the encrypted content, (KD) being protected in a form obtainable by the receiver;

the transmitter obtaining the content encrypted according to (KD) to result in (KD(content)), and sending (KD(content) to the receiver;

the receiver receiving the session response and (KD(content)), retrieving the policy and the protected content key (KD) for decrypting the encrypted content from the session response, confirming that the policy allows the receiver to render the content, obtaining the content key (KD), applying (KD) to (KD(content)) to reveal the content, and then in fact rendering the content in accordance with the policy.

2. The method of claim 1 comprising:

the transmitter in conjunction with sending the session response also storing at least a portion of the session request and at least a portion of the session response in a transmitter session store;

the receiver receiving the session response from the transmitter and storing at least a portion of the session response in a receiver session store;

the receiver retrieving at least a portion of the session response from the receiver session store, and sending a transfer request to the transmitter based on the session response; and

the transmitter receiving the transfer request and retrieving the at least a portion of the session request and at least a portion of the session response from the transmitter store based on the transfer request, retrieving from the retrieved at least a portion of the session request and at least a portion of the session response the identification of the content, obtaining the content encrypted according to (KD) to result in (KD(content)), and sending a transfer response to the receiver including (KD(content)).

3. The method of claim 1 comprising the receiver sending the session request further including a version number of a revocation list of the receiver (V-RL-R), and the transmitter sending the session response further including a version number of a revocation list of the transmitter (V-RL-X), the method further comprising the receiver determining that (V-RL-R) is more current than (V-RL-X) and sending the revocation list thereof to the transmitter.

4. The method of claim 1 comprising the receiver sending the session request further including a version number of a revocation list of the

receiver (V-RL-R), and the transmitter determining that a version number of a revocation list thereof (V-RL-X) is more current than (V-RL-R) and sending the revocation list thereof to the receiver.

5. The method of claim 1 comprising the receiver sending a session request to the transmitter including a public key of the receiver (PU-R) and the transmitter sending a session response to the receiver including the content key (KD) for decrypting the content encrypted according to (PU-R).

6. The method of claim 1 comprising the receiver sending a session request to the transmitter including a public key of the receiver (PU-R) and the transmitter sending a session response to the receiver including a seed from which the content key (KD) for decrypting the content may be derived, the seed being encrypted according to (PU-R).

7. The method of claim 1 wherein the transmitter has a public-private key pair (PU-X, PR-X), and further comprising the transmitter obtaining the content key (KD) from the license as (PU-X(KD)), applying (PR-X) to (PU-X(KD)) to result in (KD), and then re-encrypting (KD) according to a public key of the receiver (PU-R) to result in (PU-R(KD)), the receiver decrypting the content key by applying a private key (PR-R) corresponding to (PU-R) to (PU-R(KD)) to result in (KD).

8. The method of claim 1 comprising the transmitter sending a session response to the receiver further including a signature / MAC generated based on such session response, the signature / MAC binding the policy to the session response.

9. The method of claim 8 comprising the transmitter sending a session response to the receiver including a signature / MAC based on a

symmetric integrity key (KI), the session response further including (KI) encrypted according to a public key of the receiver (PU-R) to result in (PU-R(KI)), the method also comprising the receiver receiving the session response from the transmitter, retrieving (PU-R(KI)) therefrom, applying a private key (PR-R) corresponding to (PU-R) to (PU-R(KI)) to result in the (KI), and verifying the signature / MAC of the session response based on (KI).

10. The method of claim 8 comprising the transmitter sending a session response to the receiver including a signature / MAC based on a symmetric integrity key (KI) derivable from a seed, the session response further including the seed protected according to a public key of the receiver (PU-R) to result in (PU-R(seed)), the method also comprising the receiver receiving the session response from the transmitter, retrieving (PU-R(seed)) therefrom, applying a private key (PR-R) corresponding to (PU-R) to (PU-R(seed)) to result in the seed, deriving (KI) from the seed, and verifying the signature / MAC of the session response based on (KI).

11. The method of claim 1 further comprising the receiver registering with the transmitter by:

the receiver sending a registration request to the transmitter, the registration request including the unique identification of the receiver;

the transmitter validating the registration request;

the transmitter sending a registration response to the receiver, the registration response including a registration ID generated by the transmitter to identify the registration response, and the unique identification of the receiver;

the receiver sending a port address of a port thereof and the registration ID to the transmitter;

the transmitter sending a proximity message to the receiver by way of the sent port address and concurrently noting a start time;

the receiver upon receiving the proximity message at the port address thereof employing at least a portion of the registration response and the proximity message to generate a proximity value and sending a proximity response with the proximity value to the transmitter; and

the transmitter receiving the proximity response with the proximity value from the receiver and concurrently noting an end time, verifying the proximity value based on the first and second nonces, calculating from the noted start and end times an elapsed time, comparing the elapsed time to a predetermined threshold value, deciding from the comparison that the receiver satisfies a proximity requirement, and registering the receiver as being able to access content from such transmitter.

12. The method of claim 11 comprising the receiver sending a registration request to the transmitter including a digital certificate provided to the receiver by an appropriate certifying authority, the certificate including therein a public key of the receiver (PU-R) and a digital signature, the method also comprising the transmitter validating the certificate and verifying with reference to a revocation list that the certificate has not been revoked.

13. The method of claim 11 comprising the receiver sending a registration request to the transmitter including a device ID of the receiver.

14. The method of claim 11 comprising the receiver sending a registration request to the transmitter including a public key of the receiver (PU-R), and comprising the transmitter encrypting at least a portion of the registration response by (PU-R) and the receiver decrypting the registration response by application of a private key (PR-R) corresponding to (PU-R).

15. The method of claim 11 comprising:

the transmitter sending the registration response including a first nonce to the receiver;

the transmitter sending the proximity message with a second nonce to the receiver by way of the sent port address and concurrently noting the start time;

the receiver upon receiving the proximity message at the port address thereof employing the sent first and second nonces to generate the proximity value and sending the proximity response with the proximity value and the registration ID to the transmitter.

16. The method of claim 15 comprising the receiver generating a proximity value by employing the first nonce as a cryptographic key to perform an encryption of the second nonce and thus result in an encrypted value.

17. The method of claim 15 comprising the receiver generating a proximity value by employing the first nonce as a cryptographic key to perform a hash over the second nonce and thus result in a hash value.

18. The method of claim 15 comprising the receiver generating a proximity value by performing a hash over the first and second nonces to result in a hash value.

19. The method of claim 11 comprising the transmitter registering the receiver by placing the unique identification of the receiver in a registry list, and determining from the unique identification of the receiver in the session request with reference to the registry list that the receiver is in fact registered to the transmitter.

20. The method of claim 11 comprising the transmitter periodically requiring the receiver to re-register by re-sending a registration request to the transmitter.